CLAIMS

1. In a distributed network of interconnected computing devices, a network virus monitor, comprising:

a virus sensor operable in a number of modes arranged to detect a computer virus in the network such that the bandwidth of the network is substantially unaffected in a first mode wherein when the virus sensor detects the computer virus the virus sensor switches to a second mode such that only those data packets infected by the computer virus are not returned to the network.

2. A monitor as recited in claim 1, further comprising:

a traffic controller coupled to the virus sensor and the network arranged to select certain data packets wherein the selected data packets are forwarded to the virus sensor.

3. A monitor as recited in claim 2, wherein the traffic control unit further comprises:

a data packet copier operable in the first mode arranged to generate a copied data packet of each of the selected data packets wherein the selected data packets are returned to the network.

4. A monitor as recited in claim 3 wherein the data packet copy unit is disabled in the second mode such that the selected data packets are passed to the virus sensor unit.

5. A monitor as recited in claim 4, wherein the virus monitor further comprises:

a data packet protocol identifier coupled to the virus sensor unit arranged to identify a data packet protocol associated with the data packet infected by the computer virus.

6. A monitor as recited in claim 5, wherein the selected data packets are each associated with the data packet protocol associated with the computer virus such that only those data packets associated with the identified data packet protocol are selected from the network.

7. A monitor as recited in claim 1 wherein the virus sensor unit further comprises:

a filescan module arranged to scan a selected file for the computer virus.

8. A monitor as recited in claim 7, wherein the filescan unit is remotely located.

9. A monitor as recited in claim 8, wherein the remotely located filescan unit is used for scan large selected files.

10. A method of monitoring a distributed network of computing devices for a computer virus, comprising:

at a virus monitor coupled to the distributed network;

monitoring a flow of data packets in the network for the computer virus without substantially reducing the flow of data packets thereby preserving network bandwidth in a standby mode;

determining that at least one of the monitored data packets is infected with the computer virus; and

monitoring the flow of data packets such that the infected data packets are not returned to the flow of data packets in an inline mode based upon the determining.

11. A method as recited in claim 10, further comprising:

isolating a portion of the network infected by the computer virus; and

cleaning the isolated portion of the network.

12. A method as recited in claim 10, further comprising:

sending a virus report to a controller.

13. A method as recited in claim 10, further comprising:

copying selected ones of the flow of data packets from corresponding original data packets retrieved from the flow of data packets based upon a packet type; and

returning the retrieved data packets to the flow of data packets.

14. A method as recited in claim 13, wherein the packet type is determined by the detected computer virus.

15. A method as recited in claim 14, wherein a network bandwidth associated with the standby mode is substantially unaffected by the monitoring.

16. A method as recited in claim 14, wherein a network bandwidth associated with the inline mode is reduced by the infected data packets that are not returned to the flow of data packets.

17. Computer program product for monitoring a distributed network of computing devices for a computer virus, comprising:

at a virus monitor coupled to the distributed network capable of executing computer code,

computer code for monitoring a flow of data packets in the network for the computer virus without substantially reducing the flow of data packets thereby preserving network bandwidth in a standby mode;

computer code for determining that at least one of the monitored data packets is infected with the computer virus;

computer code for monitoring the flow of data packets such that the infected data packets are not returned to the flow of data packets in an inline mode based upon the determining; and

computer readable medium for storing the computer code.

18. Computer program product as recited in claim 17, further comprising:

computer code for isolating a portion of the network infected by the computer virus; and

computer code for cleaning the isolated portion of the network.

19. Computer program product as recited in claim 17, further comprising:

computer code for sending a virus report to a controller.

20. Computer program product as recited in claim 17, further comprising:

computer code for copying selected ones of the flow of data packets from corresponding original data packets retrieved from the flow of data packets based upon a packet type; and

computer code for returning the retrieved data packets to the flow of data packets.

21. Computer program product as recited in claim 20, further comprising:

computer code for determining the packet type using the detected computer virus.

22. Computer program product as recited in claim 21, wherein a network bandwidth associated with the standby mode is substantially unaffected by the monitoring.

23. Computer program product as recited in claim 21, wherein a network bandwidth associated with the inline mode is reduced by the infected data packets that are not returned to the flow of data packets.